SKIPJACK VALIDATION LIST

3/2/2000

The purpose of this document is to provide technical information about implementations of the SKIPJACK algorithm that have been validated as conforming to certain specifications in Federal Information Processing Standard Publication 185, *Escrowed Encryption Standard (EES)* and FIPS PUB 81, *DES Modes of Operation.* The SKIPJACK algorithm is referenced in FIPS PUB 185, and specified in the R21 Technical Report entitled "SKIPJACK" (S), R21-TECH-044-91. The National Institute of Standards and Technology (NIST) has made every attempt to provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, NIST cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list.

SKIPJACK Algorithm Validated Implementations

The list below describes SKIPJACK implementations which have been validated using the tests found in the NIST Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*. The implementations are validated in accordance with FIPS 185 and FIPS 81, *DES Modes of Operation.* This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories.

The list is ordered numerically, according to the certificate number. Also indicated after the date of validation are the modes and states (encryption(e) and/or decryption(d)) for which the implementation was validated. The various modes are abbreviated as follows: *Electronic Codebook* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), and *Output Feedback* (OFB). The certificate issued to the vendor indicates the CMT laboratory that tested the implementation.

#	Vendor	Skipjack Implementation	Module Type	Validation Date	Validated Modes / Description
4	**SPYRUS Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick TEL: (410) 964-6400 FAX: (410) 964-5154 info@spyrus.com	**Rosetta Smart Card, v 2.01**	**Hardware**	2/24/2000	**ECB (e/d)** An ISO 7816 compliant public key smart card based on the SPYCOS card operating system.
3	**SPYRUS Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick TEL: (410) 964-6400 FAX: (410) 964-5154 info@spyrus.com	**LYNKS Privacy Card**	**Firmware**	7/19/1999	**ECB (e/d); CBC (e/d); CFB (e/d; for 64 bits of feedback only); OFB (e/d)** PCMCIA based cryptographic token supporting symmetric algorithms, random number generation, key generation, and signature capabilities.
2	**Mykotronx** 357 Van Ness Way Torrance, CA 90501 -Blane Yamamoto TEL: (310) 533-8100 FAX: (310) 533-0527	**MYK-82 Chip**	**Hardware**	4/1/1997	**ECB (e/d)** The MYK-82 is a VLSI microcircuit.

1	**SPYRUS Inc.** 5303 Betsy Ross Drive Santa Clara, CA 95054 http://www.spyrus.com -Bill Bialick TEL: (410) 964-6400 BBialick@spyrus.com	**FORTEZZA Crypto Card, Version 0.2**	**Hardware**	12/12/1996	**ECB (e/d)**